Enterprise Risk Management
The New 2017 Version

It's all about Strategy and Performance

UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

COURSE OF BUSINESS AUDITING
UNIVERSITY OF ROME TOR VERGATA

NOVEMBER 2021

PROF FABIO ACCARDI

ERM Framework 2017 Enterprise Risk Management–Integrating with Strategy and Performance

In September 2017, the Committee of Sponsoring Organizations of the Treadway Commission (#COSO) issued the much-awaited update to the 2004 ERM–Integrated Framework, one of the most widely recognized and applied risk management frameworks in the world (COSO, 2017)

- Authored by PwC
- Reflects the evolution of ERM thinking and practices
- Links the risk management approach with the fundamental business model and process.

WHY a new Version:
The Changing Business and Risk Landscape

Bob Hirth, COSO (2017) Chair was quoted:

"The complexity of risk has changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting

Our overall goal is to continue to encourage a risk conscious culture."

Profuse changes have been evident in the way we do business and new forces are can rapidly alter the risk landscape

Growing complexity of governance, risk, and control

The new Framework provides the fundamental understanding of the chemistry among risk, performance, strategy, and value.
It is designed to turn a preventative, process-based risk monologue into a proactive, opportunities-focused conversation
to uncover how risk management can create, preserve and realize value

What ERM is?

The new framework lucidly clarifies what ERM is — and isn't. The value of true ERM is that it promotes an enterprise wide approach and understanding of risk

What IS

It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with the purpose of managing risk in creating, preserving, and realizing value

WHAT IS Not

Enterprise risk management is not a function or department.

It cannot be relegated to a checklist of tasks

What's new?
The key highlights from the Framework

10 Things to Know about the Framework

1 Provides a New Document Structure focused on fewer components (five)

2 Introduces Principles (20 key principles within each of the five components)

3 Incorporates new graphics with stronger ties to the business model

4 Focuses on integration (Integrating ERM with business practices)

5 Emphasizes Value (how entities create, preserve, and realize value)

6 Links to Strategy (Explores strategy from three different perspectives)

7 Links to Performance (Enables the achievement of strategy by actively managing risk and performance)

8 Recognizes Importance of Culture NY ExplorING the possible effects of culture on decision making

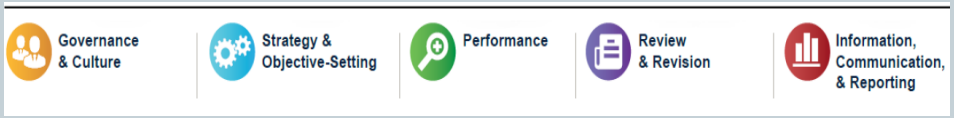
9 Focuses on Decision-making (how enterprise risk management drives risk aware decision making)

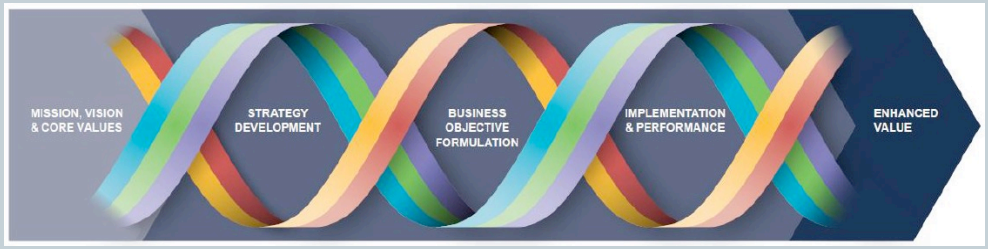
10 Builds links to internal control (The two frameworks are distinct and complementary)

Components and Principles of Risk Management

The Framework is focused on five easy-to-understand components of risk management and follows the business model versus an isolated risk management process:

1. Governance and culture
2. Strategy and objective-setting
3. Performance
4. Review and revision
5. Information, communication, and reporting





Components and Principles of Risk Management: Governance & Culture

An entity's board of directors plays an important role in governance and significantly influences enterprise risk management. Where the board is independent from management and generally comprises members who are experienced, skilled, and highly talented, it can offer an appropriate degree of industry, business, and technical input while performing its oversight responsibilities. In fulfilling its role of **providing risk oversight**, the board challenges management without stepping into the role of management. Another critical influence on enterprise risk management is culture. **The culture reflects the entity's core values:** the beliefs, attitudes, desired behaviors, and importance of understanding risk. Culture supports the achievement of the entity's mission and vision.

Components and Principles of Risk Management: STRATEGY & OBJECTIVE SETTING

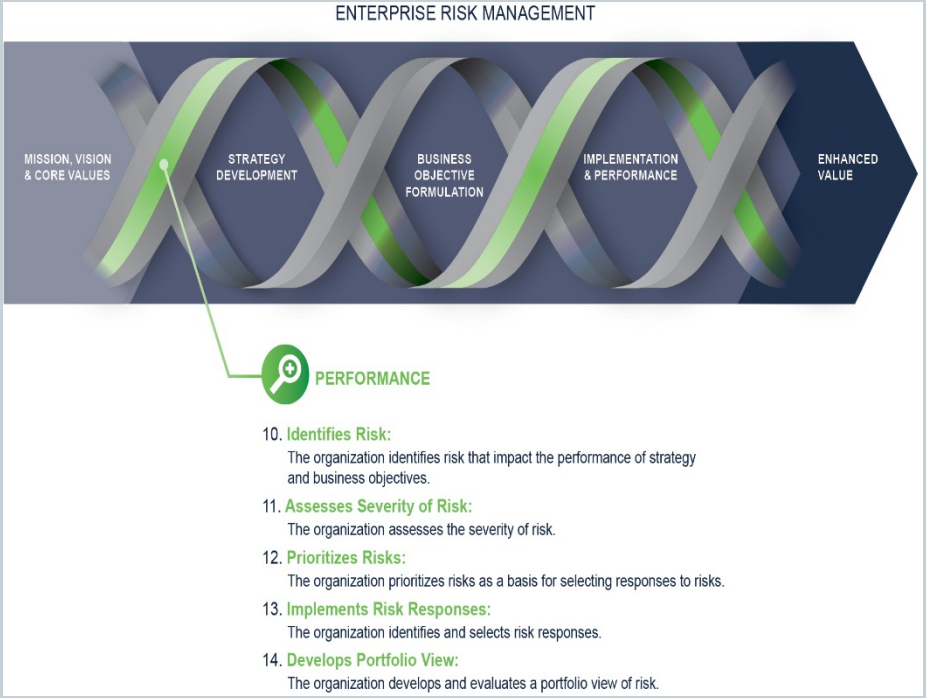
- Every entity has a strategy for bringing its mission and vision to fruition, and to drive value.
- It can be a challenge to assess **whether the strategy will align with mission, vision, and core values**, but it is a challenge that must be taken on.
- **By integrating enterprise risk management with strategy-setting, an organization gains insight into the risk profile associated with strategy and the business objectives.**
- Doing so guides the organization and helps to sharpen the strategy and the tasks necessary to carry it out.

Components and Principles of Risk Management: PERFORMANCE

- Creating, preserving, realizing, and minimizing the erosion of an entity's value is further enabled by **identifying, assessing, and responding to risk that may impact the achievement of the entity's strategy and business objectives**.

- Risks may be **highly correlated** with factors within the business context or with other risks. Further, risk responses may require significant investments in infrastructure or **may be accepted as part of doing business**

- It focuses on practices that support the organization in making decisions. Organizations use their operating structure to develop a practice that:
- **Identifies** new and emerging risks so that management can deploy risk responses in a timely manner.
- **Assesses** the severity of risk, with an understanding of how the risk may change depending on the level of the entity.
- **Prioritizes risks**, allowing management to optimize the allocation of resources in response to those risks.
- Identifies and selects **responses to risk**.



Components and Principles of Risk Management: Review and Revision

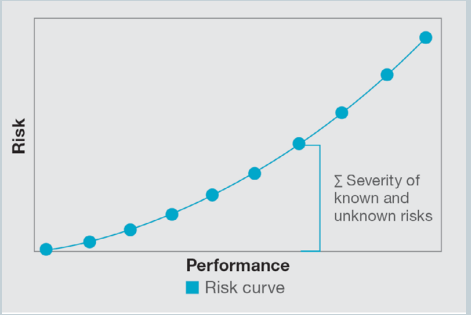
- An entity's strategy or business objectives and enterprise risk management practices and capabilities **may change over time** as the entity adapts to shifting business context.
- In addition, the business context in which the entity operates can also change, **resulting in current practices no longer applying or sufficient** to support the achievement of current or updated business objectives.
- As necessary, **the organization revises its practices or supplements it capabilities**

Components and Principles of Risk Management: Information, Communication, and Reporting

- Advances in technology and business have resulted in **exponential growth in volume of, and attention on, data**. Organizations today are challenged by the enormous quantity of data and the speed at which it all must be processed, organized, and stored.
- In this environment, it is important that organizations **provide the right information, in the right form, at the right level of detail, to the right people, at the right time.**
- Organizations **transform data into information** about stakeholders, products, markets, and competitor actions.
- Through their communication channels, they can **provide timely, relevant information** to targeted audiences.

stronger ties to the business model

- The new Framework follows the business model rather than an alien risk management process.



- The new guidance makes it clear that risk management starts with objectives - strategic and operational.
  - **WITHOUT A RELEVANT OBJECTIVE, THERE CAN BE NO RISKS**
- What this new COSO guidance means is that hundreds of thousands, perhaps millions of organizations around the world that have used risk registers as a foundation for their ERM efforts ("risk-centric ERM") need to transition to objective centric ERM

A Multidimensional Focus in Strategy-Setting

- Many institutions focus on identifying risks to the execution of the strategy. However, ERM 2017 asserts that "**risks to the strategy**" is not the only dimension of risk to consider strategically. There are two additional dimensions to consider in strategy-setting that can significantly affect an enterprise's risk profile:

1. The possibility of strategy and business objectives not aligning with mission, vision and values that define what it is trying to achieve and how it intends to conduct business. A misaligned strategy increases the possibility that, even if successfully executed, the enterprise may not realize its mission and vision

2. The implications from the strategy chosen: When managers develop a strategy, they work through alternatives and make decisions on the tradeoffs. Each alternative strategy has its own risk profile. It needed to consider how the strategy works in tandem within the organization's risk appetite, and how it will help drive the organization to set objectives and ultimately allocate resources efficiently.

- ERM is as much about understanding the implications from the strategy and the possibility of strategy not aligning as it is about managing risks to the implementation of the strategy and business objectives

Focuses on integration for better information

- Integrating ERM with business practices results in better information that supports improved decision-making and leads to enhanced performance.

It helps organizations to:	Anticipate risks
	Identify and pursue opportunities
	Respond to deviations in performance quickly
	Develop and report a portfolio view of risk
	Improve collaboration, trust, and information sharing
	Enables risk aware decisions

It's all about performance

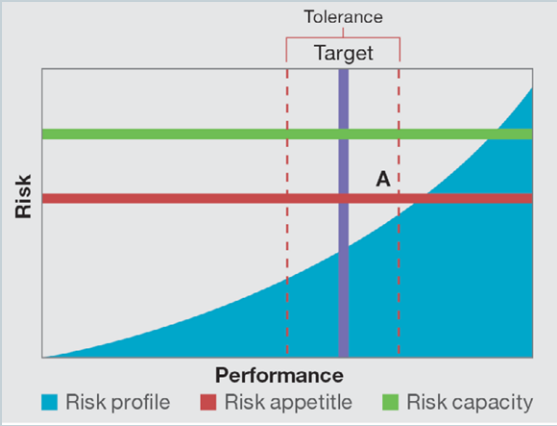
- One challenge for management is to determine **how much uncertainty – and therefore how much risk – the organization is prepared and able to accept**.

- Effective ERM allows management to **balance exposure against opportunity**, with the goal of enhancing capabilities to create, preserve and ultimately realize value.

The new framework enables the achievement of strategy by actively managing risk and performance.

Risk is integral to performance:

- Risks that impact performance must be identified and assessed;
- Risks is a variation in performance
- Organization should know how much variation can be tolerated
- Risk should be managed in the context of achieving strategy and business objectives – not as individual risks.
- More risks could be suitable if it result in a better performance
- Organization should make risk aware decisions by selection the proper risk profile, aligned with the risk appetite



Key concepts: Risk appetite

- It is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value. The first expression of risk appetite is an entity's mission and vision. Risk Appetite should be considered in strategic-planning: it allows to select, among different strategic options and related objectives, those that ensure **alignment with the mission and the vision**

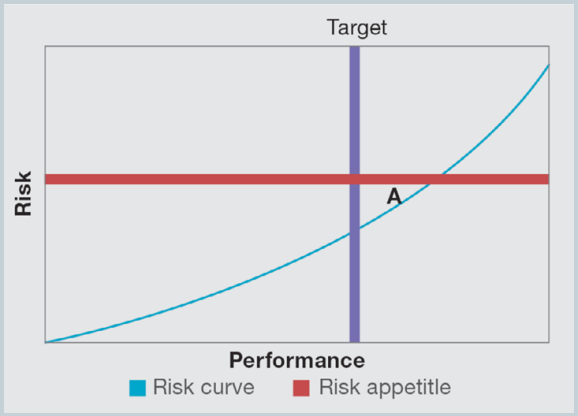
Risk appetite is not a static concept: it must be flexible enough to allow the organization to adapt to changes in the internal and external context.

It can be considered the highest trust agreement between the company and its stakeholders and it must therefore be aligned with the related expectations.

The choice of the desired risk appetite is a strategic decision itself:

- right level of risks must be weighted with the level of performance in line with the objectives of creating value.

This aspect can best be understood comparing risk appetite with risk capacity

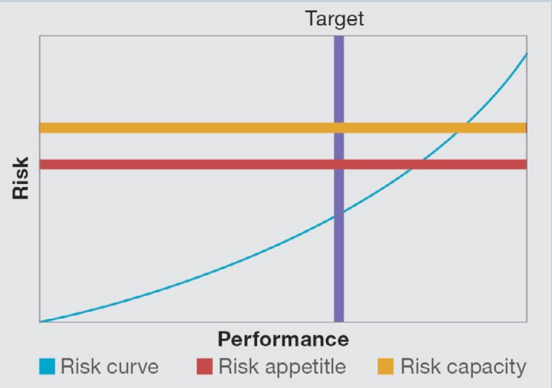


Key concepts: Risk capacity

- It is the maximum amount of risk an entity is able to absorb in the pursuit of strategy and business objectives, taking into account the structure of its capital, or the regulatory context.

- It is the limit beyond which the risk appetite cannot be fixed without exposing the organization to the danger of failing.

If risk appetite is very high, but its risk capacity is not large enough to withstand the potential impact of the related risks, the entity could fail



On the other hand, if the entity's risk capacity significantly exceeds its risk appetite, the organization may lose opportunities to add value for its stakeholders through better and more courageous performance.

Key concepts: Tolerance

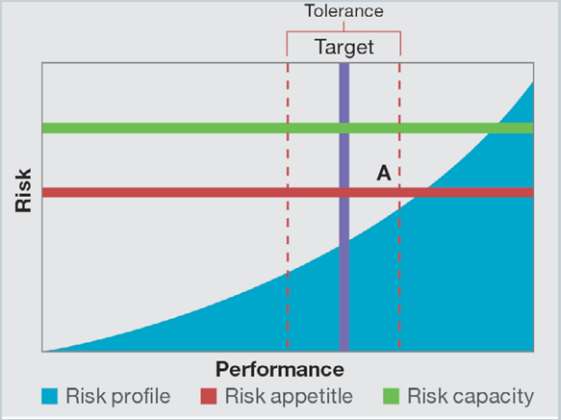
- Closely linked to risk appetite is tolerance—the **acceptable variation in performance**. It describes the range of acceptable outcomes related to achieving a business objective within the risk appetite. It also provides an approach for measuring whether risks to the achievement of strategy and business objectives are acceptable or unacceptable.

- Unlike risk appetite, which is broad, tolerance is tactical and focused.

Tolerance is as well an indicator (Key Risk Indicators - KRI - or Key Performance Indicators - KPI) that provides information on whether the organization is in the right track, prusuing to its plans, objectives or strategies or if there are warning flags that require corrective actions.

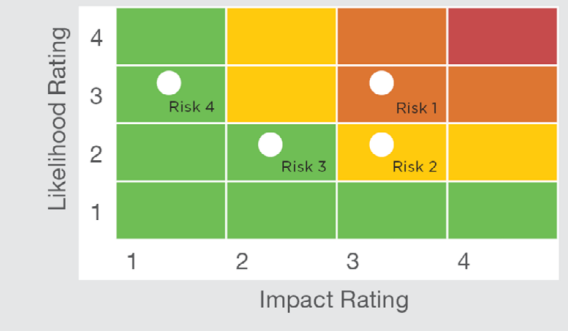
Tolerance is specific to each objective and must be measured in the same as performance.

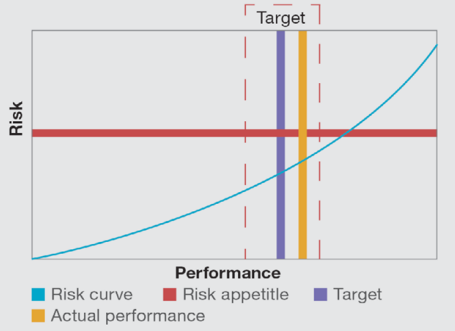
Each action or decision has a risk: it is important to pursue it being aware of risks and monitoring tolerance thresholds.



Key concepts: risk profile

- Any strategic or decision-making option has an impact on entity risk profile.
- Management must assess and anticipate the impacts on the overall risk profile of the company deriving from the strategic plans chosen, adapting it to the objectives that are to be achieved in the process of creating sustainable value. Once the objectives have been defined and the risks associated with them are identified, the organization can use the assessments on its risk profile in order to better understand the intrinsic relationship between the existing risks, the desired performance and the current one.
- Overall, risk profile provides information on the current risk exposure at the different levels of the organization, it can also be represented in the form of a register with the value of risks. All control measures are aimed at maintaining the chosen risk profile.





Key concepts: Inherent, Target, and Residual Risk

Inherent risk

Is the risk to an entity in the absence of any direct or focused actions by management to alter its severity

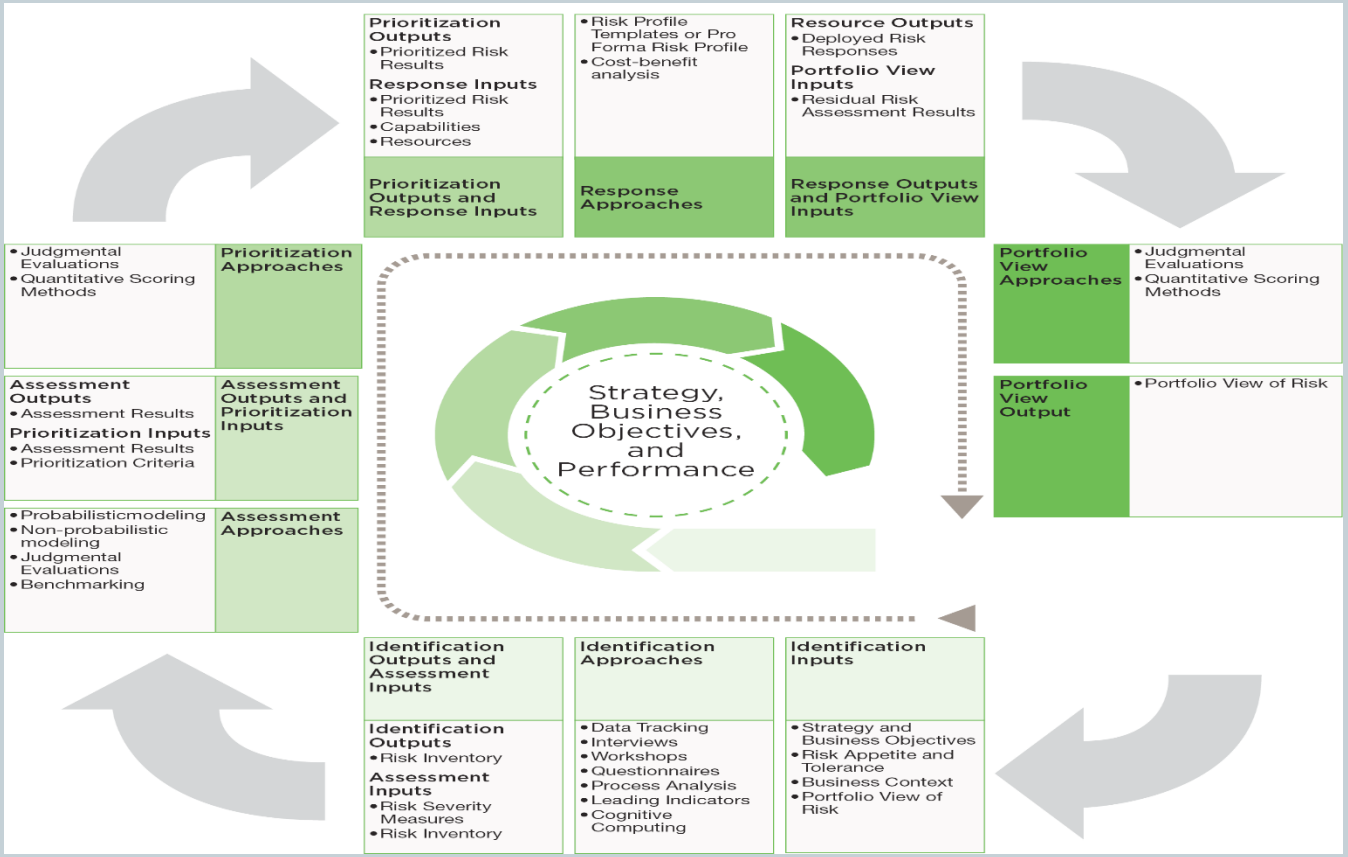
Target residual risk

Is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.

Actual residual risk

Is the risk remaining after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk. Where actual residual risk exceeds target risk, additional actions should be identified that allow management to alter risk severity further

Risk management cycle



Risk prioritization

- Organizations prioritize risks in order to inform decision-making on risk responses and optimize the allocation of resources. Given the resources available to an entity, management must evaluate the trade-offs between allocating resources to mitigate one risk compared to another. The prioritization of risks, given their severity, the importance of the corresponding business objective, and the entity's risk appetite helps management in its decision-making.

- **Adaptability**
  The capacity of an entity to adapt and respond to risks (e.g., responding to changing demographics such as the age of the population and the impact on business objectives relating to product innovation).

- **Complexity**
  The scope and nature of a risk to the entity's success. The interdependency of risks will typically increase their complexity (e.g., risks of product obsolescence and low sales to a company's objective of being market leader in technology and customer satisfaction)

- **Velocity**
  The speed at which a risk impacts an entity. The velocity may move the entity away from the acceptable variation in performance. (e.g., the risk of disruptions due to strikes by port and customs officers affecting the objective relating to efficient supply chain management)

- **Persistence**
  How long a risk impacts an entity (e.g., the persistence of adverse media coverage and impact on sales objectives following the identification of potential brake failures and subsequent global car recalls)

- **Recovery**
  The capacity of an entity to return to tolerance (e.g., continuing to function after a severe flood or other natural disaster). Recovery excludes the time taken to return to tolerance, which is considered part of persistence, not recovery

Risk responses

- For all risks identified, management selects and deploys a risk response. Management considers the severity and prioritization of the risk as well as the business context and associated business objectives

- **Options:**

Accept

- No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite. Risk that is outside the entity's risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies

Avoid

- Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity

Pursue

- Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance

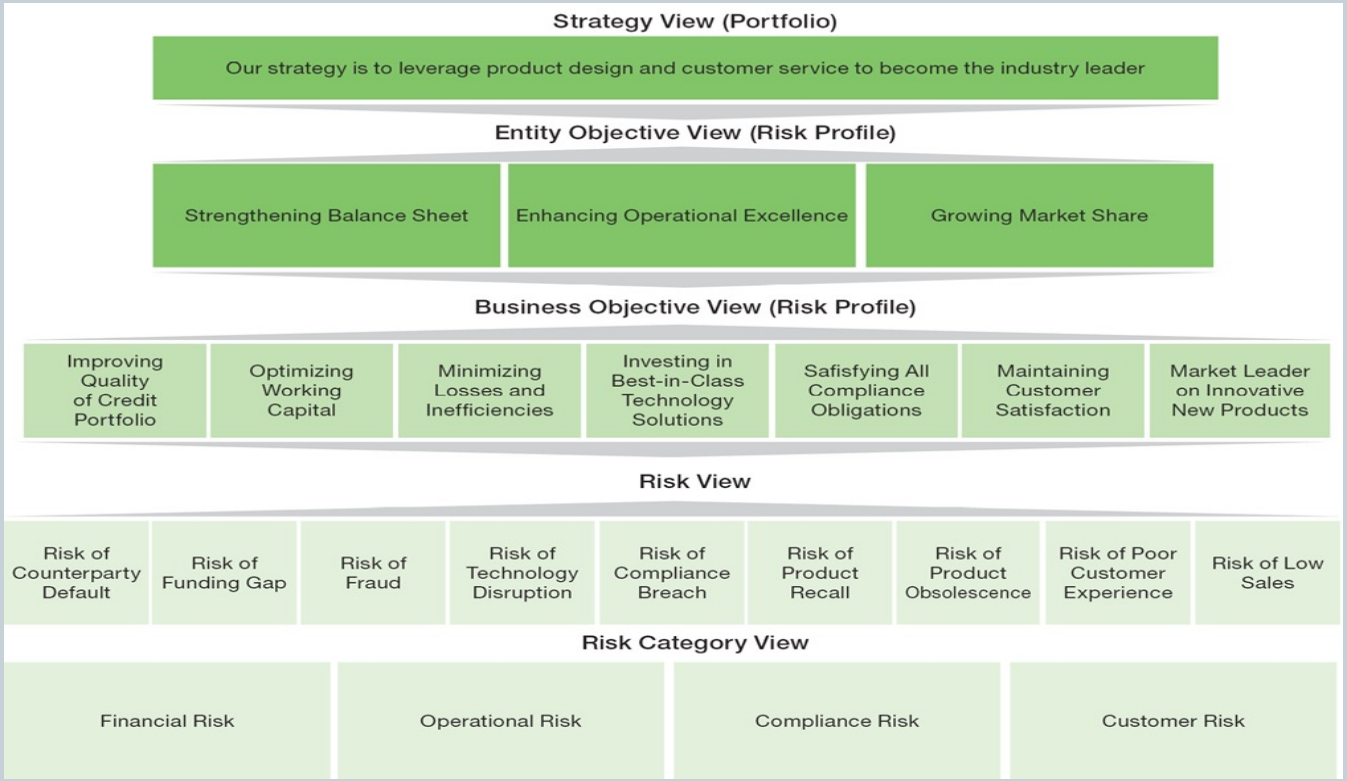
Reduce

- Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduces risk to an amount of severity aligned with the target residual risk profile and risk appetite

Share

- Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist service providers, purchasing insurance products, and engaging in hedging transactions. As with the reduce response, sharing risk lowers residual risk in alignment with risk appetite

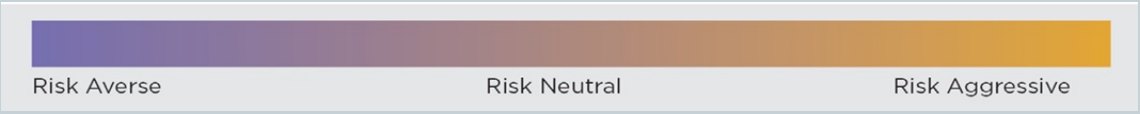
Portfolio View of risks



Importance of Culture

- ERM 2017 recognizes **Importance of Culture**

- ✓ Addresses the growing focus, attention and Importance of culture within enterprise risk management
- ✓ Influences all aspects of enterprise risk management
- ✓ Explores culture within the broader context of overall core
- ✓ Depicts culture behavior within a risk spectrum
- ✓ Explores the possible effects of culture on decision making
- ✓ Explores the alignment of culture between individual and entity behavior



links with internal control

- ✓ The document does not replace the Internal Control – Integrated Framework 2013
- ✓ The two frameworks are distinct and complementary, with neither superseding the other
- ✓ Both use a components and principles structure
- ✓ Aspects of internal control common to enterprise risk management are not repeated
- ✓ Some aspects of internal control are developed further in this framework
- ✓ Internal control is positioned within the Updated Document as a fundamental aspect of enterprise risk management.
- ✓ The updated document will focus on requisite areas that go beyond internal control; however, the Internal Control–Integrated Framework remains a viable and suitable framework for designing, implementing, and conducting and assessing the effectiveness of internal control and for reporting, as required in some jurisdictions.